

SUBCHAPTER H—CLAUSES AND FORMS

PART 3052—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

Subpart 3052.1—Instructions for Using Provisions and Clauses

Sec.

3052.101 Using part 3052.

Subpart 3052.2—Texts of Provisions and Clauses

3052.204–70 Security requirements for unclassified information technology resources.

3052.209–70 Prohibition on contracts with corporate expatriates.

3052.209–71 Reserve Officer Training Corps and military recruiting on campus.

3052.209–72 Disclosure of conflicts of interest.

3052.211–70 Index for specifications.

3052.211–90 Bar coding requirement (USCG).

3052.213–90 Evaluation factor for Coast Guard performance of bar coding requirement (USCG).

3052.215–70 Key personnel or facilities.

3052.216–70 Evaluation of offers subject to an economic price adjustment clause.

3052.216–71 Determination of award fee.

3052.216–72 Performance evaluation plan.

3052.216–73 Distribution of award fee.

3052.216–74 Settlement of letter contract.

3052.217–90 Delivery and shifting of vessel (USCG).

3052.217–91 Performance (USCG).

3052.217–92 Inspection and manner of doing work (USCG).

3052.217–93 Subcontracts (USCG).

3052.217–94 Lay days (USCG).

3052.217–95 Liability and insurance (USCG).

3052.217–96 Title (USCG).

3052.217–97 Discharge of liens (USCG).

3052.217–98 Delays (USCG).

3052.217–99 Department of Labor safety and health regulations for ship repair (USCG).

3052.217–100 Guarantee (USCG).

3052.219–70 Small business subcontracting program reporting.

3052.219–71 DHS mentor-protégé program.

3052.219–72 Evaluation of prime contractor participation in the DHS mentor-protégé program.

3052.222–70 Strikes or picketing affecting timely completion of the contract work.

3052.222–71 Strikes or picketing affecting access to a DHS facility.

3052.222–90 Local hire (USCG).

3052.223–70 Removal or disposal of hazardous substances—applicable licenses and permits.

3052.223–90 Accident and fire reporting (USCG).

3052.228–70 Insurance.

3052.228–90 Notification of Miller Act payment bond protection (USCG).

3052.228–91 Loss of or damage to leased aircraft (USCG).

3052.228–92 Fair Market value of aircraft (USCG).

3052.228–93 Risk and indemnities (USCG).

3052.231–70 Precontract costs.

3052.236–70 Special provisions for work at operating airports.

3052.237–70 Qualifications of contractor employees.

3052.237–71 Information technology systems access for contractors.

3052.237–72 Contractor personnel screening for unclassified information technology access.

3052.242.70 Dissemination of information—educational institutions.

3052.242–71 Dissemination of contract information.

3052.242–72 Contracting officer's technical representative.

3052.245–70 Government property reports.

3052.247–70 F.o.b. origin information.

3052.247–71 F.o.b. origin only.

3052.247–72 F.o.b. destination only.

AUTHORITY: 41 U.S.C. 418b (a) and (b).

SOURCE: 68 FR 67871, Dec. 4, 2003, unless otherwise note.

Subpart 3052.1—Instructions for Using Provisions and Clauses

3052.101 Using part 3052.

(b) Numbering.

(2)(i) Provisions or clauses that supplement the FAR.

(A) Agency-prescribed provisions and clauses permitted by HSAR and used on a standard basis (*i.e.*, normally used in two or more solicitations or contracts regardless of contract type) shall be prescribed and contained in the HSAR. OEs desiring to use a provision or a clause on a standard basis shall submit a request containing a copy of the clause(s), justification for its use, and evidence of legal counsel review to the CPO in accordance with (HSAR) 48 CFR 3001.304 for possible inclusion in the HSAR.

(B) Provisions and clauses used on a one-time basis (*i.e.*, non-standard provisions and clauses) may be approved by the contracting officer, unless a higher level is designated by the OE. This authority is subject to:

(1) Evidence of legal counsel review in the contract file;

(2) Inserting these clauses in the appropriate sections of the uniform contract format; and

(3) Ensuring the provisions and clauses do not deviate from the requirements of the FAR and HSAR.

Subpart 3052.2—Text of Provisions and Clauses

3052.204-70 Security requirements for unclassified information—technology resources.

As prescribed in (HSAR) 48 CFR 3004.470-4 Contract clauses, and (HSAR) 48 CFR 3037.110-70 (a) and (b), insert a clause substantially the same as follows:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (DED 2003)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission. The security requirements include, but are not limited to, how the Department of Homeland Security's sensitive information is to be handled and protected at the Contractor's site, (including any information stored, processed, or transmitted using the Contractor's computer systems), the background investigation and/or clearances required, and the facility security required. This requirement includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public, (*e.g.* such as bypassing a firewall).

(b) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and a certification that all DHS information has been purged from any contractor-owned system used to process DHS information. Organizational elements shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(c) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*), and the Government Information Security Reform Act of 2000, and the Federal Information Security Management Act of 2002. The plan shall meet IT security requirements in accordance with Federal policies and procedures that include, but are not limited to OMB Circular A-130, Management of Federal Information Resources, Appendix III, and Security of Federal Automated Information Resources;

(d) Within ___ days after contract award, the contractor shall submit for approval an IT Security Plan. This plan shall be consistent with and further detail the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will be according to the criteria of the Homeland Security Information Technology Security program Publication, DHS MD 4300.Pub., Volume I, Policy Guide, Part A, Sensitive Systems, which is available from the Contracting Officer upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The